TRUSTED
COMPUTER SOLUTIONS

# SecureOffice® Trusted Workstation™ Administrator Training

## Module One: Course Overview/Trusted Solaris Review

Trusted Computer Solutions, Inc.
2350 Park Center Drive, Suite 500
Herndon, VA 20171 USA
+1.703.318.7134 (Phone)
+1.703.318.5041 (Fax)
www.TrustedCS.com

# SecureOffice® Trusted Workstation™ (TWS) Administrator

- Course Agenda
  - Trusted Solaris Review – Module One
  - TCS Administrator Tools – Module Two
  - SecureOffice Administrator Tools – Module Three
  - System Administration Tasks – Module Four

# SecureOffice TWS Administrator

- Trusted Operating System Overview
  - Roles (RBAC)
  - Profiles (Principle of Least Privilege)
  - DAC (Discretionary Access Controls)
  - MAC (Mandatory Access Controls)

- Trusted Operating System Overview
  - Administrative Roles
    - Concept
      - A role is assumed from the Trusted Path
      - A role is comprised of administrative functions
      - The concept of separation of roles assures that no one “super user” is able to circumvent the system’s security measures.
      - Users log in as themselves and then assume the role.
      - Never attempt to log in as a role.  Roles are not able to directly login to the system.  An administrative user must login and then assume an administrative Role.

# SecureOffice TWS Administrator

- Administrative Roles (con’t)
  - Trusted Solaris provides you with four administrative roles
    - root
      - not the same as the plain UNIX root user
    - secadmin
    - admin
    - oper
  - An administrative user is normally assigned one of the above roles; this implies the need for 4 administrative users.

# SecureOffice TWS Administrator

- Administrative Roles (con’t)
  - root role
    - Responsible for setting up and configuring the system at installation (since no other roles exist at that point)
    - Runs the TCS provided System Administration Tools to set up/maintain the system.
    - Reviewing the audit data
    - Backing up and Recovering NIS+ maps
    - Controlling which functions can be performed by the secadmin

# SecureOffice TWS Administrator

- Administrative Roles (con’t)
  - secadmin role
    - Assigning passwords and clearance levels to users
    - Assuring proper information and sensitivity labels are present on all data in the system
    - Assuring proper DAC information is associated with all data in the system
    - Controlling the audit mechanism
    - Controlling which functions can be performed by the administrator, operator, root, and users.

# SecureOffice TWS Administrator

- Administrative Roles (con’t)
  - admin role
    - General system administration
    - Creating user accounts
    - Responsibilities for day-to-day operation of the system that should not be performed by normal users

# SecureOffice TWS Administrator

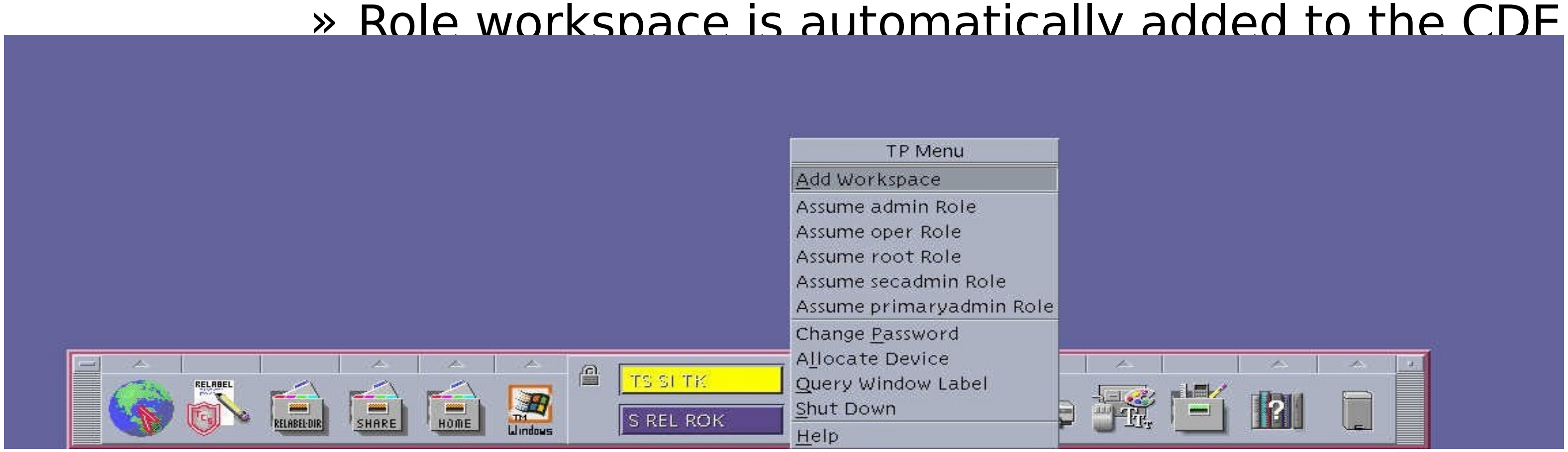
- Administrative Roles (con’t)
  - oper role
    - Performs backups (not capable of backing up MLDs)
    - None of the actions performed by oper require the Trusted Path.

# SecureOffice TWS Administrator

- Administrative Roles (con’t)
  - primaryadmin role
    - Backup for the root role
    - Disabled by default, if required contact TCS for further assistance

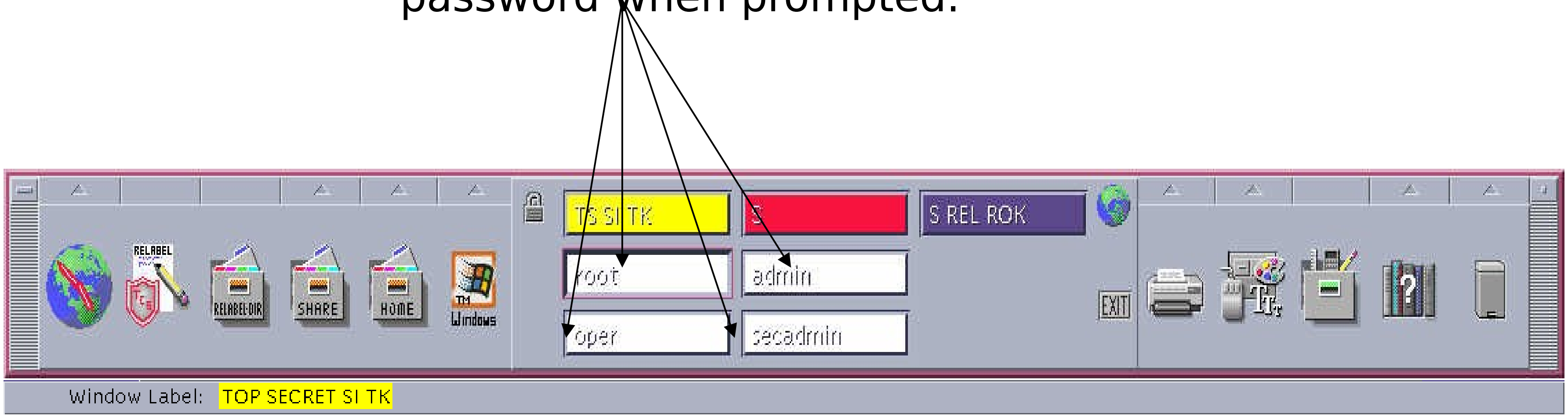
# SecureOffice TWS Administrator

- Administrative Roles (con’t)
  - Assuming  an administrative role
    - Log in to the system as a user authorized to assume the desired role.
    - Add role workspace to CDE panel
      - » Right click on the middle portion of the CDE Front Panel to bring up the Trusted Path Menu
      - » Select Role to assume (admin, root, oper, secadmin)
      - » When prompted, enter the role password
      - » Role workspace is automatically added to the CDE



# SecureOffice TWS Administrator

- Administrative Roles (con’t)
  - Assuming an administrative role (con’t)
    - Access existing role in a CDE panel workspace
      - » Left click on role workspace, enter appropriate password when prompted.



Window Label: TOP SECRET SI TK

# SecureOffice TWS Administrator

- Profiles
- A profile is a collection of
  - Actions
    - Desktop Items which can be clicked on to run programs
  - Commands
    - Processes which are run within a terminal window
  - Authorizations
    - Privileges for users; sometimes programs check for these.  The Trusted File Relabeler is one example.
- Each action or command within a profile may have
  - effective UID, GID, min and max SL to run at, and (inheritable) privileges to run.
  - Inheritable privileges allow a command or action to run with specific privileges that the specific role or user may not normally have.
- Profiles are managed with Sun’s Solaris Management Console (SMC).
- Users are assigned profiles by secadmin role in the User Tool within the SMC.

# SecureOffice TWS Administrator

- Profiles (con’t)
  - User Profile (a.k.a “rights”) Considerations
    - SecureOffice Core
    - SecureOffice NO Upgrade/Downgrade
    - SecureOffice Submitter
    - SecureOffice Processor
    - SecureOffice Downgrade ONLY
    - SecureOffice Upgrade ONLY
    - SecureOffice Upgrade/Downgrade

# SecureOffice TWS Administrator

- Profiles (cont)
  - SecureOffice Core: Basic TWS user, no relabeling rights
  - SecureOffice No Upgrade/Downgrade: Basic TWS user, no relabeling rights
  - SecureOffice Submitter: User is authorized to submit files for relabeling, cannot perform relabeler functions
  - SecureOffice Processor: User is authorized to process files for relabeling. Conducts Virus Scan, File Type Check, Dirty Word Search, Visual Review, then forwards the file bundle to an authorized Reviewer
  - SecureOffice Downgrade Only: User is an authorized Reviewer, but can only move information from a higher SL to a lower SL

# SecureOffice TWS Administrator

- Profiles (cont)
  - SecureOffice Upgrade ONLY: User is an authorized Reviewer, but is only allowed to move files from a lower SL to a higher SL
  - SecureOffice Upgrade/Downgrade: User is an authorized Reviewer, and is able to move data from any authorized SL to any authorized SL

# SecureOffice TWS Administrator

- Discretionary Access Controls (DAC)
  - Discretionary Access controls from standard UNIX.
  - Permissions for the Owner, Group and World (other) of a file
  - Read, Write, Execute permissions on a file (rwx)
    - File permissions example: -rw-r-----
      - » Bit 1 '-' (File Type: '-' represents normal file)
      - » Bit 2-4 'rw-' (Owner: Read, Write, No Execute)
      - » Bit 5-7 'r--' (Group: Read, No Write, No Execute)
      - » Bit 8-10 '---' (Others: No Read, No Write, No Execute)
  - Read, Write, Search permissions on a directory (rwx)
    - Directory permissions example: drwxr-xr-x
      - » Bit 1 'd' (File Type: 'd' represents directory)
      - » Bit 2-4 'rwx' (Owner: Read, Write, Search)
      - » Bit 5-7 'r-x' (Group: Read, No Write, Search)
      - » Bit 8-10 'r-x' (Others: Read, No Write, Search)

## Discretionary Access Controls (DAC)
## Setting DAC Permissions

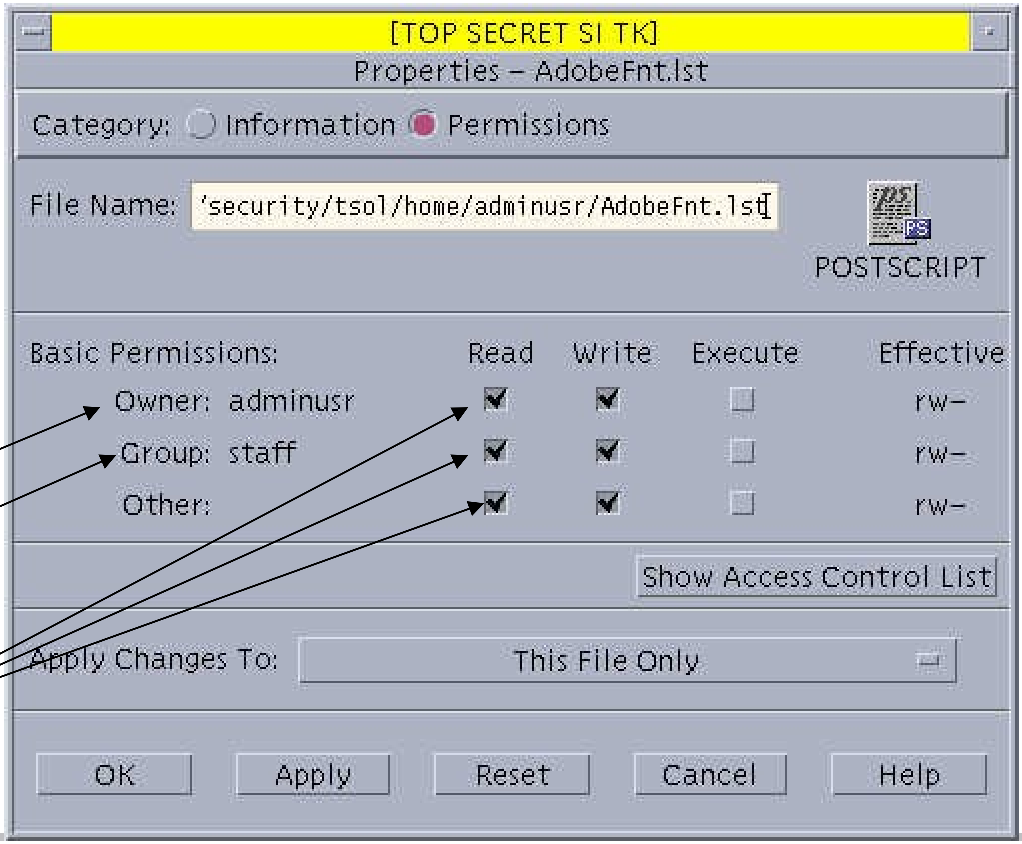
Access this file/directory properties window from file manager:

Right Click on file/directory icon, select **Properties** from the pop-up menu.

**File Owner**

**File Group**

**File Permissions**



[TOP SECRET SI TK]

Properties – AdobeFnt.lst

Category: ○ Information ● Permissions

File Name: 'security/tsol/home/adminusr/AdobeFnt.lst

Basic Permissions:

| | Read | Write | Execute | Effective |
|---|---|---|---|---|
| Owner: adminusr | ☑ | ☑ | □ | rw- |
| Group: staff | ☑ | ☑ | □ | rw- |
| Other: | ☑ | ☑ | □ | rw- |

Apply Changes To: This File Only

# SecureOffice TWS Administrator

- Mandatory Access Controls (MAC)
  - Provide the “levels” in Multi-level operating systems.
    - Subjects – Typically processes or applications running on behalf of the user
    - Objects – Typically files
  - A Subjects “level” must dominate or equal the Objects “level”
  - You can read down; read up requires a privilege
  - You can write equal; write down requires a privilege.
  - DAC and MAC access control polices are complementary.
    - A subject  that dominates an object can read down without privilege assuming that it has DAC read permissions on the object.

# SecureOffice TWS Administrator

- Trusted Solaris Review
  - Questions?

- Module Two – TCS System Administration Tools